



ADVANCED WINDOWS

Encryption

Simon Edwards gets security conscious and looks at encryption methods for your files, disks and email that will help you keep your data safe and identity thieves at bay

There are plenty of valid reasons for law-abiding citizens to encrypt their data. You don't have to be a terrorist, insider dealer, illegal pornographer or hacker to want to keep your data safe. The threat of identity theft has made us all aware of the motivation behind snoopers wanting to gather information about us, regardless of our activities.

Most of us store some level of personal information on our computers and, if that computer is ever connected to the internet, some of this information could be stolen. To criminals all over the world your internet connection is arguably more attractive than your rubbish bin as a source of personal details.

You could take a purely libertarian stance and decide that it is your right to protect your files, regardless of whether or not you have something to hide. This approach is quite sensible because, by encrypting all your files, you are not drawing special attention to a small group of them. If you simply encrypted a file or folder called Bank_Details, or Passwords.txt, an intruder to your computer would be able to focus his efforts on just a few megabytes of encrypted material. Even if he were unable to crack the encryption or was ignorant of the exact contents, he would know which files to delete to cause the maximum amount of trouble.

CODE BREAKERS

Encrypting everything is particularly important with email. If you send 100 email messages in a month and only two of them are encrypted, it doesn't take a genius to work out that those two emails will make interesting reading. Even relatively strong encryption can be broken, given enough time, effort and motivation. But if all your emails are encrypted, attackers won't be able to tell which ones are worth cracking, and breaking into all of them will probably be beyond their resources.

There are hundreds of Windows-based encryption products, including built-in software, third-party utilities and even hardware devices. Using more than one method provides defence in depth, and is advisable if you are serious about stopping unauthorised people reading your files.

If you use a firewall and anti-virus software you might think that your data is safe, but what if someone were to steal your PC? Laptops are particularly vulnerable to theft. Encrypting the hard disk will prevent thieves stealing your data, even if they have your hardware.

ENCRYPTION SOFTWARE

Windows provides a limited encryption feature. The Encrypting File System (EFS) is available on

Windows XP Professional, allowing you to encrypt files and folders by right-clicking them, choosing Properties, Advanced and then ticking the Encrypt option. The file and directory names appear in green in Explorer when encrypted.

EFS has some limitations. By default it supports the DESX algorithm (see page 260), which is weaker than 3DES (Triple DES). You can upgrade a Windows system to use 3DES, but this algorithm has been superseded by another called AES. AES is the default option with Windows XP SP1 and later. However, the way Windows implements EFS is not ideal and the inexpensive Advanced EFS Data Recovery tool from www.elcomsoft.com can decrypt EFS files and folders.

Fortunately there are other options, including a wide range of free programs as well as commercial software and dedicated encryption gadgets. Probably the most famous encryption program is PGP. This used to be free but now costs upwards of £71 for PGP Desktop Home 9. It has an easy-to-use graphical interface, integrates well with email programs such as Outlook, Outlook Express and Mozilla Thunderbird and is also compatible with some free programs including GnuPG.

GnuPG is available for many operating systems, including Windows, Linux, Mac OS X and even RISC OS. It is a command line tool, although there are graphical front ends for it. You can also download and install a plug-in that enables encryption within your choice of email program. PGP and GnuPG users can send encrypted and signed messages to each other and, if they have the correct keys, they can decrypt them too.

PGP Desktop Home 9 can create encrypted virtual hard disks, which are actually large encrypted files that appear as normal disks in Windows Explorer. You can copy files to and from this PGP Disk and, when you have finished, close it by right-clicking it and choosing PGP, Unmount. All your files are now stored safely in a single, large file that cannot be accessed

without the passphrase or, optionally, the correct private key (see below). PGP Desktop Professional 9 gives you the option of encrypting the disk in its entirety, including system files, cookies and other potentially sensitive data. A decryption key can be stored on a USB flash memory drive.

You can secure your data further by hiding it. Steganography programs such as Steganos Security Suite 2006 (www.steganos.com) can hide your encrypted data in images and sound files. This enables you to send encrypted data without alerting eavesdroppers that you are communicating an important message. Steganos Security Suite 2006 also includes the ability to encrypt emails and save files in virtual encrypted hard drives.

ENCRYPTION HARDWARE

To add a further layer of encryption, you can provide desktop PCs that use IDE hard disks with a device that automatically encrypts data as it's written to the disk. This is independent of the operating system.

You plug in a key when booting the computer and remove it once it is running. If someone turns the computer off, which they'll have to do if they want to steal either the whole unit or just the hard disk, they'll find that it is unbootable and unreadable. If they

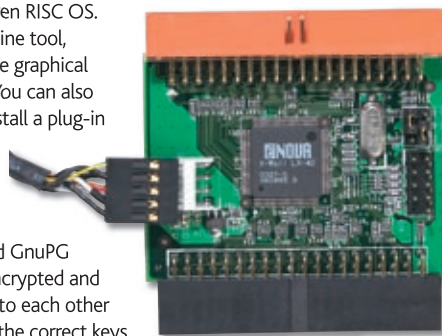
should happen to steal your key too, your PGP Disks and encrypted email messages will still protect your files. ABIT's Secure IDE is available from www.scan.co.uk/products/product_info.asp?webproductid=83552, and costs £25 including VAT.

It is good practice to keep your private encryption keys separate from the system that contains your encrypted files. If an attacker has your keys, he has won half the battle. Without them, breaking into your files is virtually impossible. This is one reason why Windows EFS can be cracked

– the keys remain on the hard disk. DESlock+ (www.deslock.com) provides a similar-looking system to EFS, where you can encrypt folders by right-clicking them. However, the encryption keys are stored on the supplied USB key, which you can back up to a spare one that's also included in the



▲ With DESlock+ you keep your encryption keys on a USB drive



▲ Encrypt your entire hard disk with ABIT's secure IDE



box. It costs £117 including VAT, and extra USB keys, known as tokens, cost just under £60 each.

SYMMETRIC v PUBLIC KEY ENCRYPTION

So far, with the exception of sending encrypted email, the encryption methods we've mentioned involve taking some data and encrypting it for your own use. This way of working generally uses symmetric encryption. If your password is strong enough and only you need access to the data, symmetric encryption is a very powerful way to keep your files private.

However, if you want to send encrypted data to someone else, perhaps by email, on a CD or even over a network, there is a better option. The problem with using symmetric encryption in cases where other people need access to the data is that you have to share a password. If you can't transmit your data securely, which is why you are using encryption in the first place, then you can't easily transmit the password. The solution is to use public key encryption.

With public key encryption each person has two sets of keys. One is a private key, which is password protected and should be stored somewhere very safe, such as on a USB key. The other is a public key, which you can distribute to anyone you want. You could even put it on your website for others to download. When someone wants to encrypt data for your eyes only, they use an encryption program such as PGP or GnuPG. This program will ask for a public key, which the sender can download and use.

Once encrypted, this data is available only to you. Even the sender cannot access it. When you receive the encrypted file your software needs access to your private key and you'll need to enter its password. The encrypted file is then decrypted and you can read the data inside. All this happens without anyone having to send a secret password across insecure channels.

Even public key encryption has vulnerabilities, the most significant of which is a man-in-the-middle attack. For this an attacker must have powerful access to your communications lines. If you sent your public key to your friend and the

attacker intercepted it, he could save it on his computer. Then he could create his own public key and send that on to your friend, posing as you. The friend would encrypt a file and send it to you, only for the attacker to intercept it. He could then decrypt this file, which is easy because it was encrypted with his public key, and read it. He could then re-encrypt it using your public key and forward the message. Neither you or your friend would be any the wiser. What you need is some way of verifying that a file has not been tampered with. This is where digital signatures come in.

SIGNATURES

Digital signatures work in a similar way to encrypting a document. The difference is that you use your private key either to encrypt the file or generate a separate signature file. If someone changes the original file and the recipient checks the signature, they will be alerted to the fact that it has been tampered with.

A man-in-the-middle attacker can get round signatures too, so this is not a solution to the scenario outlined above. But you can avoid the risk by meeting the people you want to communicate with and exchanging public keys in person. This makes it virtually impossible for an attacker to decrypt your messages and, if you sign them too, you'll know if someone has changed them.

CHOOSING AN ENCRYPTION PROGRAM

There is a wide choice of encryption products available, so how do you find out which are the best? Common but misleading marketing ploys include so-called military-grade encryption, software that supports massive encryption keys of 1,000 bits or more and "uncrackable" encryption systems that claim to contain "proprietary technology".

Let's start with the military-grade encryption. A company that makes this claim never states which military force it is talking about. It's likely that many military forces in the world have standardised on particular algorithms and key lengths for particular applications but, in itself, this is a completely meaningless claim.

The number of bits an encryption key has gives some indication as to how hard it will be to crack. Assuming that the encryption algorithm is sound (see below), you don't need massive key lengths. According to cryptography expert Bruce Schneier, keys for symmetric encryption don't need to be longer than 256 bits, and public keys of 2,048 bits are more than adequate. He says, "256-bit key lengths [are] far longer than needed for the foreseeable future. In fact, we cannot even imagine a world where 256-bit brute force searches are possible. Longer is meaningless."

You want an encryption program that supports one or more respected encryption algorithms and a reasonable range of key sizes. The Advanced Encryption Standard (AES) algorithm is the current industry standard. It is based on the Rijndael algorithm, is mathematically strong and supports key lengths of 128, 192 and 256 bits.

AES replaced DES as the industry standard but Triple DES (3DES) is expected to remain approved for use by the US government for a while yet. To put AES's strength into context, if someone could build a computer capable of cracking a DES key in a second – which would be an incredible feat involving the ability to compute and compare 2^{55} keys per second – this same computer would take 149 trillion years to crack a 128-bit AES key by brute force. If you want 'military grade' encryption, you could do worse than use AES.

Bruce Schneier has designed an encryption algorithm called Blowfish, which is free for software developers to include in their encryption programs. It is considered strong and supports key lengths of up to 448 bits. It is also a sound choice. Some encryption programs give you a choice of using 3DES, AES or Blowfish.

THINGS TO WATCH OUT FOR

Encryption can protect your data, but if an attacker can get hold of the encryption password (if you are using symmetric encryption) or the password for your private key, it's useless. Key-logging programs can spy on your computer and monitor which keys you press, in effect stealing your passwords. If an attacker has physical access to your computer his job is even easier, as inexpensive hardware key loggers are available that attach to the keyboard cable and save the keystrokes to their internal memory chips.

Even if your PC is free of key loggers, your password is still vulnerable to guesswork. Pick a good, long password that is not a dictionary word and includes numbers and punctuation and commit it to memory. If you forget it, you'll be unable to access any of your encrypted files.

Keep a backup of your encryption keys somewhere extra safe. Whatever you do, don't rely on a regular system backup. You shouldn't store your keys on the computer anyway, and if you encrypt backups using your encryption key, a system crash could leave you with backups that you cannot decrypt.

If you use Windows XP's EFS, be aware that you can designate one or more users as Data Recovery Agents. These users, who are usually Administrators, can decrypt any EFS-encrypted file on the system. This is useful if one of the other users forgets his password or leaves important documents that you need to decrypt on your computer. However, DRAs can also be a security risk. If an attacker manages to gain access to your computer using the username

ENCRYPTION ALGORITHMS

Below you'll find information on many of the block-cipher algorithms you can expect to find in commercial and free encryption programs. Some have been superseded.

3DES Triple DES uses standard DES encryption but encrypts the file three times. It uses a different key for at least one of the three encryptions, which means it has an effective key size of between 112 and 168 bits.

AES (Rijndael) The industry standard, according to the National Institute of Standards and Technology. It supports 128, 192 and 256-bit keys.

Blowfish A free encryption algorithm that supports keys from 32 to 448 bits.

CAST Patented by security company Entrust but

available for free, CAST supports 128, 160, 192, 224 and 256-bit keys.

DES With an effective key of 56 bits, the Data Encryption Standard (DES) is much weaker than 3DES or AES and is now considered out of date.

DESX A strengthened version of DES, the eXtended Data Encryption Standard was used with Windows' Encrypting File System, although later service packs replaced it with AES.

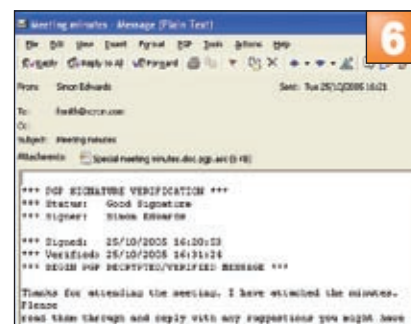
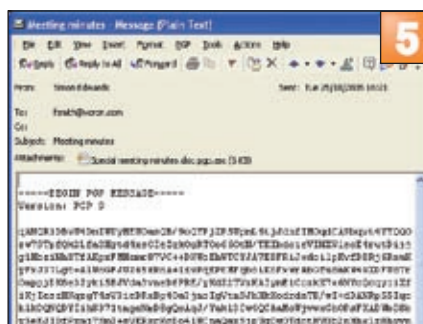
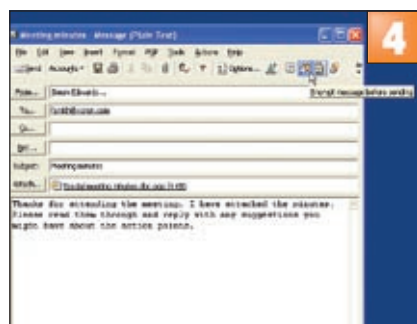
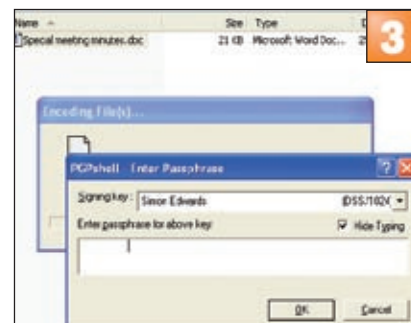
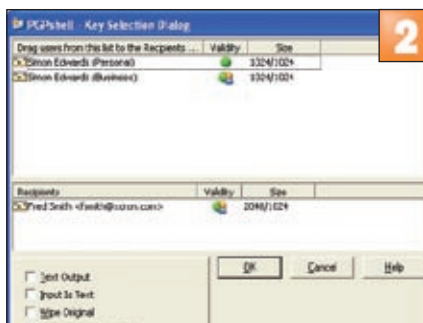
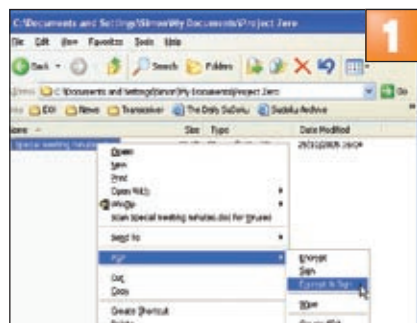
IDEA The International Data Encryption Algorithm uses 128-bit keys and is free for non-commercial use.

RSA Named after its writers, Rivest, Shamir and Adleman, RSA is a public key system that includes digital signatures and encryption.



HOW TO...

Encrypt an email using PGP and Outlook



PGP makes it easy to encrypt emails. You can download a 30-day trial version of PGP Desktop 9 from www.pgp.com to try it out. In this example, we'll assume that you have already exchanged public keys with your contact and imported his key into your keyring. This is a file that contains all the public keys of people with whom you need to exchange encrypted messages.

1 Attachments are not encrypted automatically when using PGP's Outlook plug-in, so right-click any you want to include and click PGP, Encrypt & Sign.

2 A window will appear asking who you want to encrypt the file for. It will list all the public keys you have stored in your keyring file. By default it will also encrypt the file using your own public key, which means you'll be able to decrypt it too, as well as the recipient.

Drag the recipient's entry from the list at the top to the Recipients list at the bottom. Drag your own entry from the bottom to the top unless you want to encrypt the file for yourself as well.

3 Next you need to enter your passphrase. If you were simply going to encrypt the file, this step would not be necessary because you would need only the recipient's public key, but the passphrase is required if you are going to sign a file or email because signing uses your private key.

4 Open an email in Outlook and address it as normal. The subject line won't be encrypted, so don't give away any sensitive information by using an unsuitable line such as "Here are the classified files about UFOs you wanted." Attach the documents you need, type a message and click the Encrypt button on the

toolbar. To sign the email message, click the Sign button, which is the one just to the right.

5 Press Send and, if you've chosen to sign the email, enter your passphrase again. The message is automatically encrypted, signed and sent over the internet to your contact. If anyone were to intercept it, they would see the mess in this screenshot, and would be unable to read either the message or the attachment.

6 When the recipient receives the encrypted message and its attachment he simply needs to enter his own passphrase and the email is decrypted. Double-clicking the attachment gives you the option to either open or save the attachment. Choose one then enter your passphrase to view or save the document.

and password of a DRA, he can decrypt your files. We'd advise against creating a DRA for standalone PCs unless you really know what you're doing.

Password-cracking software is available that can attempt to break into encrypted files. Sometimes these use known vulnerabilities or weakness in an encryption system, while others simply run brute force attacks by guessing every iteration of alphanumeric characters as well as running through electronic dictionaries in different languages. You can buy utilities that will crack password-protected WinZip archives and Microsoft Office documents for just a few pounds. Because

of this, using built-in password protection for these types of programs is not very secure.

Finally, don't forget that USB drives, floppy disks and, to a lesser extent, hard disks can become corrupted and stop working. If you store your private keys on a USB drive or floppy, keep a copy somewhere else as a backup. You could use the memory in your mobile phone if it can synchronise files with the PC, or simply copy them to a CD.

Get creative with your hiding places. Use steganography to hide the key in a digital photo and save the file, along with hundreds of other snaps, to a CD. Create a folder on your digital

camera's memory card or an MP3 player's disk, and use that as a hiding place. Hollow out a thick paperback novel and insert a floppy disk containing your key files. Copy your private key to any type of disc or drive and secure it at the bank. Safety deposit boxes at your high street bank can cost as little as £50 per year.

If you follow half of this advice your Windows PC will be a stronghold that frustrates the most persistent and technical of identity thieves. Encrypting your files is an easy and powerful way to protect your data, and the sooner you get around to it, the better you'll sleep. **ES**